FQ5-612   49

Claims:

1.   A data encryption system for performing
encryption/decryption of a given plain/cipher text using
transformation tables which transforms bit strings of the given
plain/cipher text, comprising:

5   a memory for storing an encryption program including
the transformation tables each of which contains a
predetermined number of entries, wherein a targeted
transformation table is previously identified from the
transformation tables depending on whether the targeted
10   transformation table exhibits a trend of increasing in the number
of operation entries as a length of encryption time becomes
longer;

a program controlled processor for executing the
encryption program;

15   a cache memory placed between the memory and the
program-controlled processor; and

an entry loading section for loading at least one
part of the targeted transformation table into the cache memory.

2.   The data encryption system according to claim 1,
20   wherein the entry loading section loads the at least one part
of the targeted transformation table into the cache memory before
the encryption/decryption of the given plain/cipher text.

3.   The data encryption system according to claim 2, wherein the entry loading section loads all transformation tables into the cache memory, wherein the targeted transformation table is loaded after the other transformation tables have been loaded into the cache memory.

5

4.   The data encryption system according to claim 2, wherein the entry loading section loads all transformation tables with priorities into the cache memory, in which a transformation table with higher priority is left longer in the cache memory, wherein higher priority is assigned to the targeted transformation table compared with the other transformation tables.

10

5.   The data encryption system according to claim 2, wherein the entry loading section loads the at least one part of the targeted transformation table into the cache memory at a plurality of timings before the encryption/decryption of the given plain/cipher text.

15

6.   The data encryption system according to claim 1, wherein the entry loading section comprises:

20   a management table containing a plurality of management entries each corresponding to the entries of the targeted transformation table, each management entry

indicating whether a corresponding entry of the targeted

transformation table has been used; and

a unused-entry manager for loading unused entries

of the targeted transformation table into the cache memory by

5   referencing the management table.

7.   The data encryption system according to claim 1,

wherein the targeted transformation table is identified by

calculating a use rate of a number of operation entries to a

total number of entries for each of the transformation tables

10   and selecting a transformation table having a smaller use rate

as the targeted transformation table.

8.   A data encryption system for performing

encryption/decryption of a given plain/cipher text using

transformation tables which transforms bit strings of the given

15   plain/cipher text, comprising:

a memory for storing an encryption program including

the transformation tables each of which contains a

predetermined number of entries;

a program-controlled processor for executing the

20   encryption program;

a cache memory placed between the memory and the

program-controlled processor; and

a cache-miss generating section for generating a

cache miss so as to make a number of cache misses uniform for

any plain/cipher text.

9.   The data encryption system according to claim 8,
wherein the cache-miss generating section comprises:

a management table containing a plurality
5   of management entries each corresponding to the entries of each
transformation table, each of the management entries indicating
whether a corresponding entry of the transformation table has
been used; and

a cache-miss generating section for generating a
10   cache miss a number of times which is equal to a difference
between a number of usable entries and a number of used entries
of the transformation table, wherein the used entries are
identified by referencing the management table.

10.   The data encryption system according to claim 8,
15   wherein the cache-miss generating section comprises:

a count management table containing a plurality
of management entries each corresponding to the entries of each
transformation table, each of the management entries indicating
a number of times a corresponding entry of the transformation
20   table has been referenced; and

a cache-miss generating section for generating a
cache miss a number of times which is equal to a number of cache
hits for the transformation table, wherein the number of cache
hits is obtained based on management entries having a count

value of at least 2.

11.   The data encryption system according to claim 10,
wherein the cache-miss generating section generates a cache miss
each time a count value of a management entry exceeding 1 is
5   incremented.

12.   The data encryption system according to claim 9,
wherein the transformation table is a targeted transformation
table which is previously identified from the transformation
tables depending on whether the targeted transformation table
10   exhibits a trend of increasing in the number of operation entries
as a length of encryption time becomes longer.

13.   The data encryption system according to claim 12,
wherein the targeted transformation table is identified by
calculating a use rate of a number of operation entries to a
15   total number of entries for each of the transformation tables
and selecting a transformation table having a smaller use rate
as the targeted transformation table.

14.   The data encryption system according to claim 10,
wherein the transformation table is a targeted transformation
20   table which is previously identified from the transformation
tables depending on whether the targeted transformation table
exhibits a trend of increasing in the number of operation entries

as a length of encryption time becomes longer.

15.   The data encryption system according to claim 14,
wherein the targeted transformation table is identified by
calculating a use rate of a number of operation entries to a
5   total number of entries for each of the transformation tables
and selecting a transformation table having a smaller use rate
as the targeted transformation table.

16.   A data encryption system for performing
encryption/decryption of a given plain/cipher text using
10   transformation tables which transforms bit strings of the given
plain/cipher text, comprising:
        a memory for storing an encryption program including
the transformation tables each of which contains a
predetermined number of entries, which includes at least one
15   transformation table group containing N transformation tables
having same contents, wherein a transformation table is
referenced N times for an encryption/decryption process of a
single plain/cipher text;
        a program-controlled processor for executing the
20   encryption program; and
        a cache memory placed between the memory and the
program-controlled processor,
        wherein, each time accessing the transformation
table group, a different one of the N transformation tables

FQ5-612   55

is referenced within the accessed transformation table group.

17.   A data encryption system for performing encryption/decryption of a given plain/cipher text using transformation tables which transforms bit strings of the given

5   plain/cipher text, comprising:

a memory for storing an encryption program including the transformation tables each of which contains a predetermined number of entries;

a program-controlled processor for executing the

10   encryption program;

a cache memory placed between the memory and the program-controlled processor;

a waiting time determination section for determining a waiting time; and

15   a time extension section for extending an encryption/decryption time for the given plain/cipher text by the waiting time.

18.   The data encryption system according to claim 17, further comprising:

20   a timer for measuring an actual encryption/decryption time for the given plain/cipher text,

wherein the waiting time is a difference between a predetermined maximum time and the actual encryption/decryption time.

FQ5-612   56

19.   The data encryption system according to claim 17, wherein the waiting time is a constant time period.

20.   The data encryption system according to claim 17, wherein the waiting time is a randomly determined time period.

5   21.   The data encryption system according to claim 17, further comprising:

a time adjustment controller for randomly determining whether time adjustment is executed,

wherein the waiting time determination section and

10   the time extension section operate only when it is determined that the time adjustment is executed.

22.   A data encryption program instructing a cache-equipped computer to perform encryption/decryption of a given plain/cipher text using transformation tables which

15   transforms bit strings of the given plain/cipher text, the program comprising the steps of:

a) generating the transformation tables each of which contains a predetermined number of entries, wherein a targeted transformation table is previously identified from

20   the transformation tables depending on whether the targeted transformation table exhibits a trend of increasing in the number of operation entries as a length of encryption time becomes

longer;

      b) loading at least one part of the targeted transformation table into a cache memory of the computer; and

      c) performing data transformation of bit strings
5 of the given plain/cipher text.

      23.   The data encryption program according to claim 22, wherein the step b) comprises the steps of:

      loading transformation tables other than the targeted transformation table into the cache memory; and
10   after having loaded the transformation tables other than the targeted transformation table, loading the targeted transformation table into the cache memory.

      24.   The data encryption program according to claim 22, wherein the step b) comprises the step of:
15   loading all transformation tables with priorities into the cache memory where a transformation table with higher priority is left longer, wherein higher priority is assigned to the targeted transformation table compared with the other transformation tables.

20   25.   The data encryption program according to claim 22, wherein the at least one part of the targeted transformation table is loaded into the cache memory at a plurality of timings before the data transformation of the given plain/cipher text.

26.   The data encryption program according to claim 22,
wherein the step b) comprises the steps of:

preparing a management table containing a plurality
of management entries each corresponding to the entries of the
5   targeted transformation table, each of which indicates whether
a corresponding entry of the targeted transformation table has
been used; and

loading unused entries of the targeted
transformation table into the cache memory by referencing
10   the management table.

27.   The data encryption program according to claim 22,
wherein the targeted transformation table is identified by
calculating a use rate of a number of operation entries to a
total number of entries for each of the transformation tables
15   and selecting a transformation table having a smaller use rate
as the targeted transformation table.

28.   A data encryption program instructing a
cache-equipped computer to perform encryption/decryption of
a given plain/cipher text using transformation tables which
20   transforms bit strings of the given plain/cipher text, the
program comprising the steps of:

a) generating the transformation tables each of
which contains a predetermined number of entries;

b) performing data transformation of bit strings of the given plain/cipher text; and

c) generating a cache miss so as to make a number of cache misses uniform for any plain/cipher text before

5   terminating the encryption/decryption.

29.   The data encryption program according to claim 28, wherein the step c) comprises the steps of:

preparing a management table containing a plurality of management entries each corresponding to the entries of each

10   transformation table, each of the management entries indicating whether a corresponding entry of the transformation table has been used; and

generating a cache miss a number of times which is equal to a difference between a number of usable entries and

15   a number of used entries of the transformation table, wherein the used entries are identified by referencing the management table.

30.   The data encryption program according to claim 28, wherein the step c) comprises the steps of:

20   preparing a count management table containing a plurality of management entries each corresponding to the entries of each transformation table, each of the management entries indicating a number of times a corresponding entry of the transformation table has been referenced; and

FQ5-612   60

generating a cache miss a number of times which is
equal to a number of cache hits for the transformation table,
wherein the number of cache hits is obtained based on management
entries having a count value of at least 2.

5   31.   The data encryption program according to claim 30,
wherein a cache miss is generated each time a count value of
a management entry exceeding 1 is incremented.

           32.   A data encryption program instructing a
cache-equipped computer to perform encryption/decryption of
10   a given plain/cipher text using transformation tables which
transforms bit strings of the given plain/cipher text, the
program comprising the steps of:
           generating the transformation tables each of which
contains a predetermined number of entries, which includes at
15   least one transformation table group containing N
transformation tables having same contents, wherein a
transformation table is referenced N times for an
encryption/decryption process of a single plain/cipher text;
and
20   performing data transformation of bit strings of
the given plain/cipher text by referencing a different one of
the N transformation tables each time accessing the
transformation table group.

33.   A data encryption program instructing a
cache-equipped computer to perform encryption/decryption of
a given plain/cipher text using transformation tables which
transforms bit strings of the given plain/cipher text, the
5   program comprising the steps of:
        generating the transformation tables each of which
contains a predetermined number of entries;
        performing data transformation of bit strings of
the given plain/cipher text;
10   determining a waiting time; and
        extending an encryption/decryption time for the
given plain/cipher text by the waiting time.

34.   A data encryption method for performing
encryption/decryption of a given plain/cipher text using
15   transformation tables which transforms bit strings of the given
plain/cipher text, the method comprising the steps of:
        a) generating the transformation tables each of
which contains a predetermined number of entries, wherein a
targeted transformation table is previously identified from
20   the transformation tables depending on whether the targeted
transformation table exhibits a trend of increasing in the number
of operation entries as a length of encryption time becomes
longer;
        b) loading at least one part of the targeted
25   transformation table into a cache memory of the computer; and

FQ5-612   62

          c) performing data transformation of bit strings
of the given plain/cipher text.

          35.   A data encryption method for performing
encryption/decryption of a given plain/cipher text using
5   transformation tables which transforms bit strings of the given
plain/cipher text, the method comprising the steps of:
          a) generating the transformation tables each of
which contains a predetermined number of entries;
          b) performing data transformation of bit strings
10   of the given plain/cipher text; and
          c) generating a cache miss so as to make a number
of cache misses uniform for any plain/cipher text before
terminating the encryption/decryption.

          36.   A data encryption method for performing
15   encryption/decryption of a given plain/cipher text using
transformation tables which transforms bit strings of the given
plain/cipher text, the method comprising the steps of:
          generating the transformation tables each of which
contains a predetermined number of entries, which includes at
20   least one transformation table group containing N
transformation tables having same contents, wherein a
transformation table is referenced N times for an
encryption/decryption process of a single plain/cipher text;
and

FQ5-612   63

performing data transformation of bit strings of
the given plain/cipher text by referencing a different one of
the N transformation tables each time accessing the
transformation table group.